A hacker group known as Rex Mundi has taken credit for infiltrating AmeriCash Advance, a payday lender. The hacking group was able to break into the system and steal customer names, email addresses, the last four digits of their Social Security numbers, and the names of their financial institutions. They threatened to release this information to the public if AmeriCash did not pay them $15,000 “idiot tax”. When the company refused to give into extortion Rex Mundi released the customer data. They claim to have motives for choosing which companies they hack; however they admit money is the key motivator.

According to the hackers statement in the article, AmeriCash was extremely negligent to not protect the area of entry. They stated that it was so obvious that it was referenced in their robots.txt file. Apparently from what I found online the robot.txt file is like a do not enter warning for robots trying to visit the site. From what I can gather from this is that they knew it was sensitive information, being that it was a robot.txt file, yet they somehow failed to protect the information. The hacking group did not say how it was insecure so I will explain a few things that should have been in place to protect the information. First, all data should have been encrypted using one of the many methods we learned in class. Finally, the website should have been SSL/TLS secured to protect from a potential breach.